FPKIMA Newsletter

Spring 2015
Volume 2 Issue 2

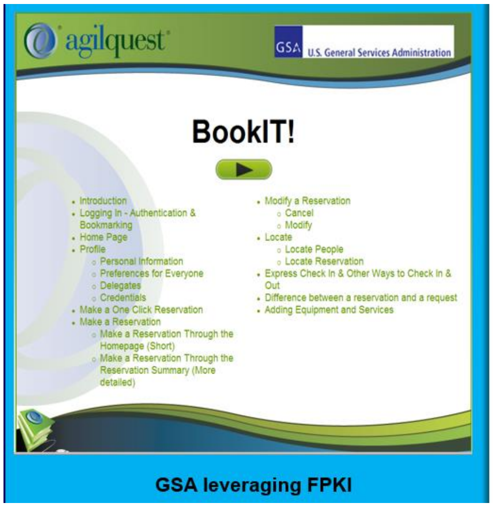
Federal PKI Management Authority
Enabling Trust

Inside This Issue

The White House approved the creation of a new cybersecurity coordination center called the Cyber Threat Intelligence Integration Center or the CTIIC. The new federal agency will be modeled after the National Counterterrorism Center and operated under the guidance of the Director of National Intelligence as a cybersecurity threat intelligence fusion center. The CTIIC will be the central point to coordinate cyber threat intelligence from the FBI, NSA, DHS, and other federal agencies while also providing cybersecurity intelligence to other departments and agencies to carry out their cybersecurity missions.

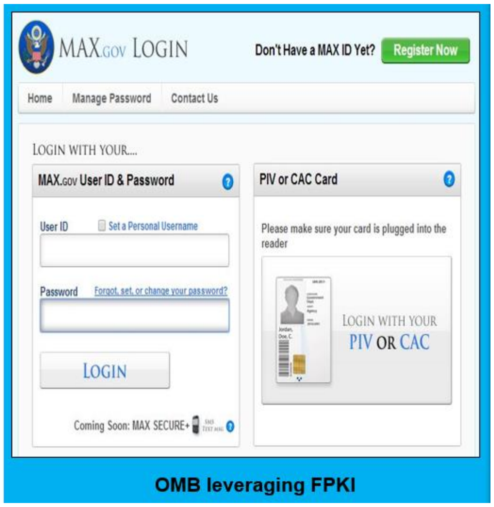
Federal Public Key Infrastructure Value

As the Federal PKI (FPKI) approaches its 15 year birthday we want to take a step back and reflect on how the FPKI has benefited the federal government, federal identity management, and commercial industry. What started as a proof of concept in a dusty basement closet is now an enterprise-grade federated identity management system serving more than 10 million users. To put that number in perspective, New York City has an estimated population of 8.5 million. The FPKI user population is spread out among federal, state, and local government, commercial industry, and foreign partners. The FPKI enables each of these entities to conduct its business with the federal government in a secure and efficient manner.



- Introduction
- Logging In - Authentication & Bookmarking
- Home Page
- Profile
  - Personal Information
  - Preferences for Everyone
  - Delegates
  - Credentials
- Make a One Click Reservation
- Make a Reservation
  - Make a Reservation Through the Homepage (Short)
  - Make a Reservation Through the Reservation Summary (More detailed)
- Modify a Reservation
  - Cancel
  - Modify
- Locate
  - Locate People
  - Locate Reservation
- Express Check In & Other Ways to Check In & Out
- Difference between a reservation and a request
- Adding Equipment and Services

GSA leveraging FPKI



Please make sure your card is plugged into the reader

OMB leveraging FPKI

Examples of Federal Agencies leveraging the FPKI for efficient operations

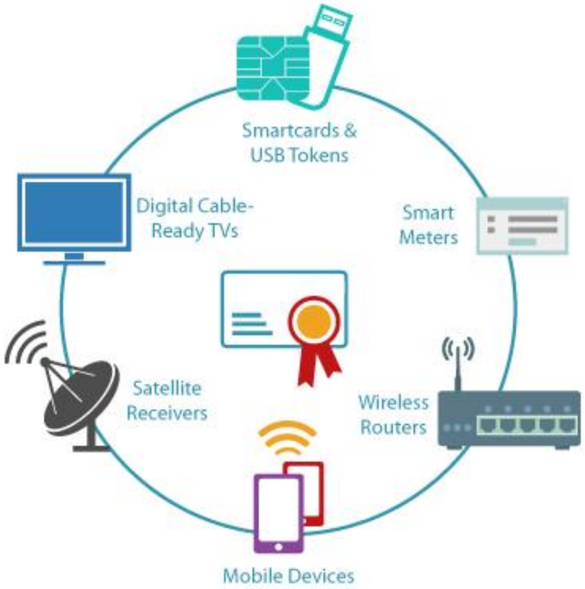
Some innovative uses of the FPKI by agencies include our very own General Services Administration (GSA) and its BookIT! Application. The GSA building at 1800 F Street was redesigned as an open concept office, removing cube farms and most private office spaces. The new open office concept is enhanced by a PKI-enabled desk reservation application that is tied to the physical access system so when an employee swipes their PIV card they are also checked in for a desk reservation if one exists.

The Office of Management and Budget (OMB) hosts a government-wide collaboration, information sharing, data collection, and analytic capability website for any cross-government and inter-agency collaboration called “OMB MAX”. OMB MAX utilizes the FPKI to allow any PIV or CAC holder simple identity verification and account registration. These are just two of the many federal and state agencies that are realizing the true value of the FPKI in their organizations. If your organization is using the FPKI we want to hear about it! Send your use cases and examples to FPKIPA-MA@listserv.gsa.gov to be included in future newsletters.

FPKI Device Certificates

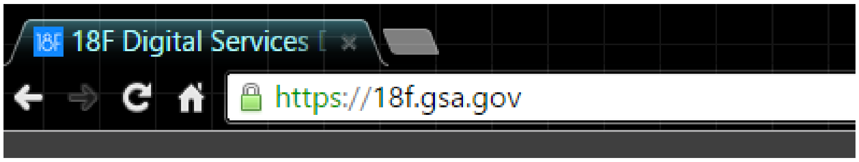
The What, Why, and How of Non-Person Certificates

Device certificates are commonly known as non-person entity or NPE certificates and can be issued to any and all types of devices and applications. In the FPKI, a device is loosely defined as anything that is not a person and can include servers, routers, mobile devices, client machines, and other components or things that require secure authentication to operate. A device certificate will provide proof and assurance of the authenticity of a device and can prevent rogue or malicious devices from interacting with your network.



Example of Devices (Source: LawTrust http://www.lawtrust.co.za)

Still confused? We use device certificates every day and probably do not realize it. The most common type of device certificate is a TLS/SSL certificate or the certificate used by an HTTPS website connection. The SSL certificate acts as both a means for the user to ensure they are at the correct website and also establishes an encrypted session to share information. Device certificates are also used in the "internet of things" or IoT which comprises all the connected devices we use on a daily basis to include not only smart phones but also smart watches, fitness trackers, and other internet-enabled devices. A more FPKI focused example are the server certificates issued from a domain controller to validate the PIV card used during logon or the certificates issued from the EGCA to application servers, identity providers, and other devices that comprise the FICAM Trust Framework. Have an interesting use of device certificates in your organization? Send it to FPKIPA-MA@listserv.gsa.gov to be included in a future newsletter.



Example of a SSL Device Certificate on a .gov website.

Did you know?

BMW uses SSL certificates to secure communications between new BMW cars and keyless entry systems. Is your agency using certificates to secure communications between devices? Tell the FPKIPA so we can improve our device certificate policies.

Did you know?

The FPKI operates a device-only certificate authority. The eGovernance CA or EGCA only issues certificates to devices and supports the FICAM Trust Framework Solutions program. This CA issues certificates to application servers, back end attribute exchange brokers, metadata servers, relying party applications, and identity providers to support SAML assertions. Want to learn more or become involved in the Federal Internet of Things (IoT)? Go to http://www.idmanagement.gov/trust-framework-solutions

Keeping your laptop and devices safe on the road is just as important as when you are in the office. Before taking that flight or hopping on the train, update your devices so they are running the latest version of applications and anti-virus software. If possible, enable tracking locators in case your device is lost or stolen and always use a passcode or password lock. Be careful when connecting to public wireless hotspots which include airport, hotel, restaurants, or coffee shops and always use "https" websites when browsing so your internet traffic is encrypted. If possible, never visit any sensitive websites (banking, personal, etc.) when connected to a public internet hot spot either. This applies to personal devices too, because a weak personal device could lead to a major enterprise breach.

News from the FPKI

Federal Cybersecurity Law Update

Last year was a busy one for the federal government in authoring new cybersecurity laws to protect both government and commercial networks. Here is a quick recap of some of those passed in the last 12 months:

- The Federal Information Security Modernization Act (FISMA) of 2014 was signed into law by President Obama on December 18, 2014. This law updates FISMA 2002 to meet the federal government's current cybersecurity needs, established real-time monitoring of federal computer networks, and enhances oversight of federal data breaches. Through DHS, it establishes a real-time monitoring of federal computer networks, and enhances oversight of federal data breaches through centralized reporting to the Federal Information Security Incident Center (FISIC). For more information, go to https://www.us-cert.gov/government-users.

- On February 13, 2015, President Obama signed an Executive Order (EO) to encourage and promote cybersecurity threat information sharing between the private sector and government. The EO encourages the development of information sharing and analysis organizations (ISAOs) to serve as conduits between the private sector and government for cybersecurity collaboration. The purpose of this EO is to strengthen the private-public partnership in protecting secure communication of the internet which is similar to the FPKI's mission of providing and protecting secure communication to the federal government and its trusted partners. For more information, go to http://www.dhs.gov/isao.

- The Cybersecurity Enhancement Act of 2014 was signed into law by President Obama on December 18, 2014. The bill provides for "an ongoing, voluntary public-private partnership to improve cybersecurity, and to strengthen cybersecurity research and development." The bill includes provisions to promote cybersecurity information sharing, create education and awareness programs and also formalizes the role of NIST in developing the voluntary Cybersecurity Framework.

FPKI Industry Day

The FPKIMA hosted an industry day on March 23rd at GSA 1800 F Street. The event featured multiple speaker sessions on the current and future capabilities of the FPKI, a question and answer session with commercial Shared Service Providers (SSP), federal relying party use cases, future of National Strategy of Trusted Identities in Cyberspace (NSTIC)/Connect.gov, and PKI bridge capabilities. Executives and IT Managers in attendance gained a unique understanding of what the FPKI has to offer and how the FPKI can meet their cybersecurity needs.

If you missed the industry or want a copy of the presentations, they will be available on idmanagement.gov or by sending an email to FPKIPA-MA@listserv.gsa.gov.

Federal PKI Management Authority
Enabling Trust

FPKI Technical Working Group

The FPKI Technical Working Group (TWG) held a March meeting to discuss high speed Physical Access Control Systems (PACS) lessons learned, PIV smart card logon lessons learned, and an Apple mobile device manager (MDM) vulnerability. Highlights include:

- The Department of Defense (DoD) presented lessons learned from a proof of concept for a high speed PACS. They were able to achieve significant speed enhancements from using an Elliptical Curve Cryptography (ECC) issued Card Authentication Key (CAK) for a "touch and go" turn style pilot with the Washington Metro Area Transit Authority (WMATA). This pilot utilized the Common Access Card (CAC) as a WMATA fare card without comprising the security of the card or certificates.
- DoD also presented one method for mapping either multiple smart cards to a single account (operations center use case) and one smart card to multiple user accounts (system administrator use case). This method was achieved through using the security hint to identify the account to be used.
- DoD also presented a vulnerability to the Apple Over the Air registration process when deploying certificates to Apple devices with an MDM. The vulnerability has been reported to Apple, but no action has been taken at the time of this newsletter.

For more information or to be added in the FPKI TWG listserv, send an email to FPKIPA-MA@listserv.gsa.gov.

Ask the FPKIMA

What is the difference between a medium device and medium hardware certificate?

The main difference between a medium device and a medium hardware certificate is what type of person or non-person (i.e. thing) will be using the certificate. Device certificates are issued to non-person entities or NPE which are used by web servers, application servers, or other devices (things) which are not people. Medium hardware certificates are also issued to devices, but those devices are used by people such as smart cards, smart tokens, or other hardware based cryptographic devices. It is easy to get the two confused since devices can also use smart cards or smart tokens. Also, medium refers to the level of assurance (LOA) of the certificate which in this case means LOA 3 identity proofing for certificate issuance and subscriber responsibilities in protecting their private key.

Where Can I Find More Information on the FPKIMA?

Information on the FPKIMA can be found on the idmanagement.gov website below:

FPKIMA - http://idmanagement.gov/federal-public-key-infrastructure-management-authority

Need Help?

Contact the FPKIMA

FPKIPA-MA@listserv.gsa.gov

Did you know...?

Major internet browsers are implementing new security-related user interface changes without informing users or website owners. These changes include special warning screens, degraded page viewing, and other changes that affect browsing. In some instances, your browser may totally block the website and not allow you to visit the webpage. Don't worry, it's not your computer, but the intent is proactive security against malicious content. Be aware of what websites you visit and what security mechanisms they use to protect your browsing experience.